Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

Список литературы

1. Криптология / Ю. С. Харин [и др.]. – Минск: БГУ, 2013. – 512 с.
2. Holst, L. Asymptotic normality and efficiency for certain goodness-of-fit tests / L. Holst // Biometrika. – 1972. – №59. – P. 137–145.
3. Харин, Ю. С. Теория вероятностей, математическая и прикладная статистика / Ю. С. Харин, Н. М. Зуев, Е. Е. Жук. – Минск: БГУ, 2011. – 463 с.
4. Палуха, В. Ю. Статистические тесты на основе оценок энтропии для проверки гипотез о равномерном распределении случайной последовательности / В. Ю. Палуха // Весці НАН Беларусі. Серыя фізіка-матэматычных навук. – 2017. – № 1. – С. 79–88.
5. Палуха, В. Ю. Энтропийные характеристики двоичных последовательностей в криптографии / В. Ю. Палуха, Ю. С. Харин // Комплексная защита информации. Материалы XX научно-практической конференции. Минск, 19–21 мая 2015 г. – Минск: РИВШ, 2015. – С. 99–102.
6. Speedtest-500MB.bin [Electronic resource] // Humboldt Berlin University, Faculty of Mathematics and Natural Sciences, Department of Physics. – Mode of access: http://qrng.physik.huberlin.de/files/speedtest-500MB.bin. – Date of access: 08.04.2016.

ПРОГНОЗИРОВАНИЕ ДВОИЧНЫХ ВРЕМЕННЫХ РЯДОВ НА ОСНОВЕ МЕТОДА ИМИТАЦИИ ОТЖИГА

В.В. ПЬЯНОВ, Ю.С. ХАРИН

НИИ прикладных проблем математики и информатики БГУ

Введение. Случайные последовательности и их генераторы являются неотъемлемыми элементами современных криптосистем[1]. Случайные последовательности используются для построения гаммы в поточных криптосистемах, сеансовых и других ключей в блочных криптосистемах. Отметим, что для криптографических приложений требуются равномерно распределенные случайные последовательности значительной длины. Поэтому возникает важная задача статистического тестирования таких последовательностей. Одним из направлений статистического тестирования является проверка свойства невозможности прогнозирования выходных последовательностей криптографических генераторов статистическими методами. В данной статье представляется эффективный вычислительный алгоритм статистического прогнозирования, основанный на нахождении оптимального шаблона прогнозирования в классе малопараметрических цепей Маркова высокого порядка на основе метода имитации отжига.

Математическая модель временного ряда. Пусть на вероятностном пространстве (Ω, F, P) наблюдается двоичный временной ряд

$$x = (x_1, .., x_T) \in V^T = \{0,1\}^T, x_t \in V = \{0,1\},\ t = 1, \ldots, T,$$

длины T, являющийся цепью Маркова порядка s, $s \gg 1$, обладающий следующим гипотетическим свойством:

$$\frac{1}{2} - \varepsilon \le \left| P\{x_t = j_0 | x_{t-1} = j_1, \ldots,\ x_{t-s} = j_s\} - \frac{1}{2} \right| \le \frac{1}{2},\ j_0, j_1, \ldots, j_s \in V, \quad (1)$$

где $\varepsilon \in \left[0, \frac{1}{2}\right)$ – некоторое достаточно малое число. Это свойство означает, что при некотором достаточно большом s в выходной последовательности $\{x_t\}$ криптографического генератора существует статистически значимая зависимость глубины s. Прогнозированию подлежит последующий бит $x_{T+1} \in V$.

Так как распределение вероятностей, входящее в (1), на практике неизвестно, а его статистическое оценивание имеет вычислительную сложность порядка $O\left(2^{s+1}\right)$, то необходимы другие подходы к прогнозированию, использующие малопараметрические модели цепи Маркова высокого порядка[1-4]. Выберем в качестве такой модели цепь Маркова порядка s с r частичными связями[2].

Пусть $r \in \mathbb{N}, 1 \le r \le s$ – число связей, $M = \{m_1, m_2, \ldots, m_r\}$ – целочисленный r-вектор с упорядоченными компонентами $1 \le m_1 \le m_2 \le \ldots \le m_r \le s$, который будем называть шаблоном, $P = (p_{j_0,\ldots,j_{s-1},j_s}), j_0, \ldots, j_s \in V$ – $(s+1)\times(s+1)$ матрица вероятностей одношаговых переходов цепи Маркова x_t:

$$p_{j_0,\ldots,j_{s-1},j_s} = P\{x_t = j_0 | x_{t-1} = j_1, \ldots, x_{t-s} = j_s\},$$

$Q = (q_{j_0,\ldots,j_{r-1},j_r}), j_0, \ldots, j_r \in V$ – некоторая $(r+1)\times(r+1)$ стохастическая матрица.

Цепь Маркова $x_t \in V$ принято называть цепью Маркова s-го порядка с r частичными связями и обозначать ЦМ(s,r), если ее вероятности одношаговых переходов допускают следующее малопараметрическое представление:

$$p_{j_0,\ldots,j_{s-1},j_s} = q_{j_0,j_{m_1},\ldots,j_{m_r}},\ j_0, \ldots, j_s \in V.$$

В дальнейшем будем полагать, что двоичный временной ряд $x = (x_1, .., x_T) \in V^T = \{0,1\}^T$, $x_t \in V = \{0,1\}, t = 1, \ldots, T$, является цепью Маркова s-го порядка с r частичными связями.

Алгоритм прогнозирования на основе метода имитации отжига. Выберем $r \in \mathbb{N}, 1 \le r \le s$ и зафиксируем произвольный упорядоченный набор r номеров координат шаблона $M = \{m_1, m_2, \ldots, m_r\}$, где $1 \le m_1 \le m_2 \le \ldots \le m_r \le s$. Введем в рассмотрение условную вероятность события:

$$p(r, j_0, M) \rangle = P\{x_{T+1} = j_0 | x_{T-\mathrm{m}_1} = j_1, \ldots, x_{T-m_r} = j_r\},$$

где $j_1, \ldots, j_r \in V$ – фиксированные наблюдаемые значения $x_{T-m_1}, \ldots, x_{T-m_r}$. В силу (1) будем строить прогноз для x_t на основе $x_{T-m_1}, \ldots, x_{T-m_r}$. Согласно [3], оптимальная прогнозирующая статистика для модели ЦМ(s,r) примет вид:

$$\hat{x}_{T+1} = \arg\max_{j_0} p(r, j_0, M). \qquad (2)$$

Точность прогноза характеризуется величиной[3]

$$\mathrm{p}_+(r, M) \rangle = \max_{j_0 \in V} \mathrm{p}(r, j_0, M).$$

Точность прогнозирования можно увеличить, максимизируя $p_+(\cdot)$ по шаблону [4]:

$$p_+(r;M) \to \max_M . \quad (3)$$

Решением экстремальной задачи (3) будет являться набор M^* наиболее информативных компонент шаблона. Если решать задачу максимизации (3) перебором, то вычислительная сложность будет иметь порядок $O\left(C_s^r T + 2^{r+1}\right)$. Для уменьшения вычислительной сложности будем использовать метод имитации отжига (simulated annealing)[5]. Этот метод является вероятностным методом решения оптимизационных задач и основывается на имитации физического процесса кристаллизации вещества при снижении его температуры. Метод имитации отжига активно используется в задачах защиты информации[6,7].

Применяя метода имитации отжига построим следующий алгоритм прогнозирования:

Вход: $N \in \mathbb{N}$, $T \in \mathbb{N}$, $t_{\max}$, r.

Выход: $\hat{x}_{T+1}$.

Шаг 1: Случайно выбираем начальный шаблон M и вычисляем оценку для $p_+(r; j_0, M)$. Определяем «энергию» e как $e = p_+(r; j_0, M)$, и «текущую температуру» $t = t_{max}$.

Шаг 2: Случайно изменяем шаблон M, удалив из шаблона одну координату и, добавляя координату не присутствующую в шаблоне (данный шаг можно повторять для нескольких координат вместо одной), получаем измененный шаблон M'.

Шаг 3. Вычисляем оценку для $p_+(r; j_0, M')$. В случае, если $p_+(r; j_0, M') > e$, полагаем $e = p_+(r; j_0, M'), M = M'$.

Иначе с вероятностью $exp\left(-t_{max}\left(e - p_+(r; j_0, M')\right)/t\right)$, полагаем $e = p_+(r; j_0, M')$, $M = M'$.

Шаг 4. $t = t - 1$.

Шаг 5. Повторяем шаги 2 - 4 пока $t > 0$.

Шаг 6. В результате получаем $\hat{x}_{T+1} = arg\,max_{j_0 \in V}\, \hat{p}(r; j_0; M)$.

Вычислительная сложность алгоритма имеет порядок

$$W_1 = O(T\ t_{max}).$$

Результаты компьютерных экспериментов

Параметр s, означающий порядок цепи Маркова (глубину стохастической зависимости), в представленном алгоритме предполагался известным.

Для тестирования разработанного алгоритма по точности прогнозирования, характеризуемой вероятностью ошибки прогнозирования:

$$p_{\text{ош.}} = P\left\{\hat{x}_{T+1} \neq x_{T+1}\right\},$$

и вычислительной сложностью, характеризуемой затратами машинного времени $t_{маш.}$ для вычисления прогноза $\hat{x}_{T+1}$, проведены две серии компьютерных экспериментов.

В первой серии обрабатывалось 10 реализаций двоичного дискретного временного ряда длины $T = 2^{15}$, порождаемого линейной рекуррентой порядка 16:

$$x_t = x_{t-16} \oplus x_{t-14} \oplus x_{t-13} \oplus x_{t-11},$$

соответствующего модели ЦМ(s,r) при $s=16, r=4, M^* = \{11,13,14,16\}$ и удовлетворяющего свойству (1) при $\varepsilon = 0$. При $r=4, t_{max} = 1000$ прогнозирование всех 10 реализаций произошло безошибочно: $\hat{p}_{ош.} = 0;$ время обработки одной реализации составило $t_{маш.} = 0.1$ сек.

Во второй серии обрабатывалось 10 реализаций двоичного дискретного временного ряда длины $T = 2^{15}$, порождаемого нелинейной рекуррентой порядка 16:

$$x_t = x_{t-1} \oplus x_{t-2} \oplus x_{t-8}x_{t-11} \oplus x_{t-10}x_{t-16},$$

соответствующего модели ЦМ(s,r) при $s=16, r=6, M^* = \{1,2,8,10,11,16\}$ и удовлетворяющего свойству (1) при $\varepsilon = 0$. При $r=6, t_{max} = 150$ прогнозирование всех 10 реализаций произошло безошибочно: $\hat{p}_{ош.} = 0;$ время обработки одной реализации составило $t_{маш.} = 3.3$ сек.

Таким образом, компьютерные эксперименты показали эффективность разработанного алгоритма прогнозирования.

Список литературы

1. Криптология / Ю. С. Харин [и др.]. – Минск : БГУ, 2014. – 512 с.

2. Харин, Ю. С. Цепи Маркова с r-частичными связями и их статистическое оценивание / Ю. С. Харин // Доклады НАН Беларуси. — 2004. Т. 48, № 1. – С. 40–44.

3. Харин Ю.С. Оптимальность и робастность в статистическом прогнозировании: монография / Ю.С. Харин. – Минск : БГУ, 2008. – 263 с.

4. Ю. С. Харин, А. И. Петлицкий, “Идентификация двоичной цепи Маркова s-го порядка с r частичными связями при наличии аддитивных искажений”, Дискрет. матем., 22:4 (2010), 138–155

5. Aarts E. H. L., Van Laarhoven P. J. M. Simulated annealing: Theory and applications // Reidel, Dordrecht. – 1987. – Т. 9717. – С. 5.

6. Nalini N, Raghavendra Rao G, "Cryptanalysis of Block Ciphers via Improved Simulated Annealing Technique," Information Technology, 2006. ICIT '06. 9th International Conference on, Bhubaneswar, 2006, pp. 182–185.

7. Garg P. Cryptanalysis of SDES via evolutionary computation techniques //arXiv preprint arXiv:0906.5123. – 2009.

РАЗРАБОТКА ПРОГРАММНЫХ СРЕДСТВ КАТАЛОГИЗАЦИИ ФОТОАРХИВОВ

К.С. САМОЛЕТОВА

Московский технологический университет

Вследствие возрастания сложности решаемых научно-технических задач, актуализируется автоматическая обработка и анализ визуальной информации. Одной из областей интереса машинного зрения являются цифровые устройства отображения гра-